Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from One-Ring Scams	)	CG Docket No. 20-93
	)	

COMMENTS OF AT&T

Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys

June 19, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from One-Ring Scams	)	CG Docket No. 20-93
	)	

COMMENTS OF AT&T

AT&T Services, Inc.[1] ("AT&T") hereby submits these comments in response to the Commission's *Notice of Proposed Rulemaking* in the above-captioned proceeding, which proposes measures to protect consumers from one-ring scam calls.[2]

INTRODUCTION AND SUMMARY

AT&T is committed to combatting illegal and deceptive robocalls directed to its customers. In connection with this objective, AT&T monitors its network and reviews and investigates data on suspected robocall traffic on a near-continuous basis. AT&T's Global Fraud Management team then uses these data as a starting point to investigate suspicious traffic and, where permitted, block suspected illegal calls. Based on information flagged in AT&T's suspected robocall reports, AT&T routinely identifies suspected one-ring calling schemes on its network, against which AT&T takes aggressive action following careful investigation. AT&T therefore welcomes the opportunity to share its experience and to help identify steps the Commission and industry can take to better protect consumers.

In AT&T's view, the formula for addressing one-ring scams is not materially different from the steps stakeholders collectively can and should take to combat suspected illegal

---

1 AT&T Services, Inc. is filing these comments on behalf of its voice services affiliates.

2 *Protecting Consumers from One-Ring Scams*, Notice of Proposed Rulemaking, CG Docket No. 20-93, FCC 20-57 (rel. Apr. 28, 2020) ("*NPRM*").

robocalls more generally. These complementary steps can be summarized as follows: (1) deterrence; (2) detection; (3) redress, including call blocking; and (4) enforcement. To unpack the formula further, appropriate deterrence should entail, at a minimum, robust "know-your-customer" safeguards to limit the potential that a voice service provider's customers are responsible for originating illegal traffic. Detection mechanisms, by contrast, require active traffic monitoring and data analysis systems to enable the provider to identify suspected illegal traffic on its network, whether originating with the provider or from a third-party provider. Effective redress mechanisms could entail multiple components, including the development and implementation of appropriately tailored provider-initiated call blocking programs. With respect to one-ring schemes specifically, AT&T has successfully targeted such schemes using a combination of call blocking and financial redress options that can drastically limit the profitability of the schemes and, in turn, the motivation to conduct them. Finally, leveraging data from USTelecom's Industry Traceback Group ("ITG") and other sources, and consistent with Congress's directive in the TRACED Act, no effort to mitigate illegal calls of any type can be effective in the absence of robust enforcement.

The Commission possesses the authority and record necessary to encourage—and in certain cases, to require—action consistent with the foregoing framework in at least four important respects. *First*, the Commission should adopt the robocall mitigation program as proposed by USTelecom. *Second*, the time has come for the Commission to adopt a provider-initiated call blocking safe harbor. By contrast, targeted authorization to block one-ring scam calls as proposed in the FNPRM is neither necessary nor helpful. What *is* needed is a call blocking safe harbor providing sufficient legal protection to prompt more aggressive call blocking by providers. *Third* and relatedly, the Commission should consider *requiring* voice

service providers to block calls received directly from the originating or gateway providers of one-ring scams, consistent with the Commission's recent threats to address COVID-19-related scams. *Fourth* and finally, consistent with the TRACED Act, government stakeholders should identify new ways to expand coordination to bring the full force of law against illegal callers, including but not limited to, perpetrators of one-ring scams.

BACKGROUND

Although one-ring calling scams are not a new phenomenon, they are experiencing a recent resurgence as a common tool of robocall fraudsters. One-ring scams seemingly took a back seat to other forms of illegal robocalls in recent years, as robocallers leveraged cheap Voice over Internet Protocol ("VoIP") software to generate mass-calling campaigns with the intention of connecting the called consumers with live agents who often would seek to defraud or otherwise harass the called party. By contrast, one-ring scam calls are not dialed with the intention to connect the calling and called party at all—at least not with the first call. Using the same cheap technology as more traditional robocallers, one-ring callers have the ability to originate hundreds of thousands of calls per minute, each displaying a foreign (and typically spoofed) telephone number as caller ID, that then quickly disconnects before the called party has a reasonable opportunity to answer the call. The caller will place such calls to a telephone number, but with no intention of establishing communications with the called party. Instead, the sole purpose of placing the call(s) is to induce the called party to place a return call to the foreign telephone number.

When a victim of a one-ring call dials the foreign telephone number back, he or she sets in motion a string of inter-carrier and related party transactions—all involving payment—to deliver the call to its foreign destination. For example, when an AT&T customer places a return

call, AT&T routes the call to a downstream carrier with which it has a business relationship to transport traffic destined for a particular international location. The second provider may exchange the call with yet another provider. Indeed, much like domestic calls, a call destined for a foreign country may change hands multiple times prior to termination. Each provider typically pays the next provider in the call path a per-minute international settlement fee for its role in the transmitting the call. Likewise, as the originating provider, AT&T under normal circumstances would recover the expense associated with the international call from its customer, the calling party.

However, circumstances involving a one-ring call and any associated return call are far from normal. The one-ring calls themselves have very high no-answer rates—often 85 percent or higher—because the call disconnects after a single ring on the called party's device. For any one-ring calls that are answered, the average duration of the calls is very short, because the caller disconnects. Further, *return* calls may not ultimately reach their intended destination country. In recent investigations of suspected one-ring calling schemes, AT&T determined that return calls in many cases were short-stopped, either domestically or in a country other than the one with which the dialed international telephone number is associated. And when a return call connects (wherever that may occur), the victim caller often hears music, prompts from an interactive voice response ("IVR") system, or other audio content, and/or is subjected to a variety of tactics designed to keep him or her on the line for as long as possible. In so doing, the one-ring scam hits pay dirt—generating intercarrier compensation payments that ultimately flow to, or are shared with, the original caller.

DISCUSSION

I. THE COMMISSION SHOULD IMPLEMENT PROPOSALS THAT WOULD FACILITATE MORE EFFECTIVE DETERRENCE AND DETECTION OF ONE-RING SCAMS

A. The Commission Should Adopt and Apply USTelecom's Robocall Mitigation Proposal To Enhance Deterrence and Detection of One-Ring Scams.

Benjamin Franklin famously said, "an ounce of prevention is worth a pound of cure." The axiom is no less applicable in the context of illegal robocalls; the most effective tools for combatting illegal robocalls—including one-ring scams—are those that stop them at their source. For one-ring calls that terminate domestically, stopping one-ring scams at their source necessitates identification of those providers that, either unwittingly or knowingly, facilitate one-ring calling schemes through the provision of voice service to one-ring callers.

AT&T recommends adapting the robocall mitigation program proposed by USTelecom for this purpose. Indeed, although USTelecom and its members developed the robocall mitigation proposal specifically to address the TRACED Act's directive for providers subject to an extension of the STIR/SHAKEN implementation requirements, the framework contemplated under the proposal is highly versatile and adaptable to address all voice networks and types of traffic.[3] In summary, USTelecom's proposal would require voice service providers to register with the Commission and certify, among other things, that they are taking reasonable steps to avoid originating illegal robocall traffic.[4] In the event a provider is identified as the originating source of one or more one-ring calling campaigns, and in the absence of evidence that the

[3] For this reason, AT&T urges the Commission to implement an industry registration and certification process consistent with USTelecom's robocall mitigation proposal.

[4] *See* Letter from Farhan Chughtai, USTelecom, to Marlene Dortch, FCC, CG Docket No. 17-59, WC Docket No. 17-97, Attach. at 3-4 (filed Mar. 6, 2019) ("USTelecom March 6, 2020 Ex Parte").

provider has taken reasonable measures to address the problem, the Commission would take further steps to provide appropriate incentives for the provider to so act.

These additional steps likely would vary, depending on the particular circumstances and/or provider identified in connection with the one-ring scam. Indeed, such steps could take numerous forms, including—at one extreme—de-listing the provider from the proposed registry of voice service providers.[5] Such action would authorize other providers to begin blocking all calls they receive from the scofflaw provider's network, action similar to the Commission's recent aggressive efforts in coordination with the Federal Trade Commission to target gateway providers suspected of enabling COVID-19 scams.[6]

Less extreme measures should, at a minimum, include heightened robocall mitigation obligations.[7] Specifically, establishing the capability to monitor traffic patterns that would flag suspect calling campaigns, and then robust application of the provider's terms of service to eliminate problem customers should be baseline best practices for robocall mitigation for all voice providers in today's environment. Particularly for providers that become known to originate bad traffic, these obligations should be mandated, along with related reporting obligations.

B. STIR/SHAKEN and Related Proposals Are Not Viable Tools To Detect or Deter One-Ring Scams at this Time.

By contrast, AT&T opposes novel applications of STIR/SHAKEN and/or call labeling to address one-ring scams, as such proposals are premature and likely will never be sufficient. In particular, although STIR/SHAKEN, once broadly implemented, holds promise as a tool to

---

5 *See id.* at 5.

6 *See* FCC, Press Release, *FCC, FTC Demand Robocall-Enabling Service Providers Cut Off COVID-19-Related International Scammers* (May 20, 2020), https://docs.fcc.gov/public/attachments/DOC-364824A1.pdf

7 *See* USTelecom March 6, 2020 Ex Parte, Attach. at 5.

combat illegal calls that spoof domestic telephone numbers, whether providers abroad will implement the protocols is far from clear and, in any event, not on the near-term horizon. Similarly, requiring gateway (or other) domestic providers to attach C-level attestations—or particular labels—to all traffic they receive from a particular source would do little, if anything, to stem the flow of one-ring calls into the country and would require potentially burdensome and costly network implementations that are not presently on industry's roadmap. The Commission therefore should continue to allow the STIR/SHAKEN and call analytics ecosystems to mature, eschewing additional regulation to address one-ring scams until such time that the efficacy of any such requirements becomes clear.

STIR/SHAKEN is not yet a viable tool to combat one-ring scams and may never become one. As a threshold matter, the rules recently adopted by the Commission to implement the STIR/SHAKEN requirements of the TRACED Act are limited to calls using NANP telephone numbers.[8] As explained above, one-ring scams display *international* numbers as caller ID.[9] More significantly, it is far from certain if or when voice providers abroad will implement STIR/SHAKEN.[10]

Further, addressing the problem of one-ring calls underscores concerns raised in response to the proposal to require intermediate providers to sign unsigned calls they receive. Critically, STIR/SHAKEN does *not* provide a mechanism for international gateway providers (or, for that matter, any type of provider) to "verify … the nature or purpose of calls."[11] Quite simply,

---

8 *See* 47 C.F.R. § 64.6300(g); *Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 ¶ 39 (2020).

9 AT&T is not aware of any recent one-ring calling schemes using telephone numbers from other NANP jurisdictions.

10 *See NPRM* ¶ 19.

11 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. 116-105 § 12(b)(6) (2019) ("TRACED Act").

STIR/SHAKEN cannot verify caller intent.[12] And because STIR/SHAKEN cannot discern intent, requiring international gateway providers to attach a C-level attestation to all internationally originated calls would in no way advance Congress's objective in Section 12(b)(6).[13] On the contrary, by flooding the ecosystem with C-level calls, one-ring scam calls would look like any other international call, legitimate or otherwise.

In all events, reading Section 12(b)(6) of the TRACED Act so broadly as to *require* the adoption of rules applicable to *all* international gateway providers could not be tethered to any reasonable reading of the statutory language. Section 12(b)(6) directs the Commission only to "consider" whether the Commission can protect consumers from one-ring calls through regulation of international gateway providers.[14] Although AT&T supports the adoption of rules pursuant to Section 12(b)(6) in appropriate circumstances—i.e., imposing heightened know-your-customer obligations on providers identified as a domestic entry point for one-ring scams—the Commission's authority under Section 12(b)(6) plainly is limited to imposing "obligations on international gateway providers *that are the first point of entry for* … [one-ring scam] calls into the United States."[15] Appropriately read, any rules the Commission adopts pursuant to Section 12(b)(6) should be appropriately tailored to apply only to those providers identified as facilitating domestic entry of one-ring scams.

---

12 The purpose and benefit of STIR/SHAKEN is limited to determining when a call is not improperly spoofed.

13 This is particularly true for one-ring calling schemes that, notwithstanding the use of foreign telephone numbers as caller ID, originate domestically.

14 TRACED Act § 12(b)(6).

15 *Id.* (emphasis added).

II. A SAFE HARBOR FOR PROVIDER-INITIATED CALL BLOCKING PROGRAMS AND MORE AGGRESSIVE, COORDINATED ENFORCEMENT ARE NEEDED TO COMBAT ONE-RING SCAMS AND OTHER ILLEGAL CALLS

Other than adopting USTelecom's robocall mitigation proposal, call blocking is the single-most impactful tool available to service providers to combat illegal calls, including one-ring scams. Call blocking can take numerous forms. As is well-documented in the Commission's record, AT&T provides a number of customer-facing tools—most significantly, AT&T Call Protect and Digital Phone Call Protect, network-based call blocking and labeling services, which eligible customers elect to receive (or not) at no additional charge to them.[16] Separately, AT&T operates a call blocking program that targets high-volume, suspected illegal calling schemes, including one-ring scams.[17] Unlike the AT&T Call Protect suite of services, AT&T's provider-initiated call blocking program is not offered on an opt-out basis. Rather, calls blocked under the program are limited to telephone numbers that AT&T's fraud investigators have reasonably determined are being used to abuse AT&T's network to the detriment of consumers. Calls from potentially unwanted sources—such as telemarketer, survey, and other types of calls—generally are not targeted by AT&T's provider-initiated call blocking program unless their calling practices exceed thresholds that AT&T reasonably concludes are abusive and likely illegal.

AT&T has leveraged the expertise of its network analytics and fraud investigation teams to successfully target one-ring scams on its network. One-ring calling schemes share many of the same characteristics as more traditional illegal robocalling events—e.g., uncharacteristically

---

[16] *See* Letter from Joan Marsh, AT&T, to Mika Savir, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 1-4 (filed Feb. 28, 2020) ("February 28, 2020 AT&T Response"). AT&T also offers the AT&T Smart Call Blocker phone, which has call blocking capabilities and works with any landline voice service and on all wireline networks, including TDM-based telephone service, for consumers with caller ID. *Id.* at 4.

[17] *See* February 28, 2020 AT&T Response at 4-5.

high no-answer rate and very short average length of call, among other similarities. As a result, suspected one-ring scams on AT&T's network routinely are flagged on AT&T's suspected robocall report. Once identified through careful investigation, AT&T also has successfully stymied one-ring calling campaigns through a combination of defensive measures, including, for example, blocking both the inbound one-ring calls and the return calls of customers. And because one-ring scams are a form of access charge arbitrage, AT&T typically contacts its international access supplier(s) when it suspects a one-ring attack has occurred to communicate AT&T's intent to withhold payment for calls it believes to be associated with the one-ring calling scheme. Such a step is critical, as it prompts AT&T's supplier to inform any subsequent providers in the call path that payment may be denied, thus breaking the chain of payments to the party(ies) responsible for originating the one-ring scam. AT&T also often will contact the international jurisdiction whose telephone numbers were used in the attack. In AT&T's experience, the countries at issue often are unaware of the scheme—indeed, many one-ring calling schemes do not originate in the country of origin associated with the displayed caller ID—and willingly cooperate to avoid impacting the flow of legitimate traffic to and from their residents.

AT&T does not require explicit authority to block one-ring scam calls on its network. As the Commission affirmed again most recently last year, the obligation of service providers to complete calls is limited to *legal* calls.[18] Because AT&T already can (and does) lawfully block illegal one-ring calling schemes, the adoption of a one-ring-specific safe harbor would be unnecessary and superfluous. Nevertheless, such existing legal authority is insufficient to incent

[18] *Advanced Methods To Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 ¶ 23 n.53 (2019) ("*Call Blocking Declaratory Ruling*").

broader provider-initiated call blocking of one-ring scams and other illegal calls. The inevitability of a mistake dissuades providers from developing call blocking programs, or from blocking more aggressively, thus hampering the Commission's top consumer protection priority of stopping illegal calls.[19]

Voice providers need protection from liability for calls they may block in error. More specifically, voice providers such as AT&T that have *provider-initiated* call blocking programs based on criteria that the Commission has determined constitute "reasonable analytics" for *consumer-facing* call-blocking tools deserve insulation from liability for mistakes that may result from the extraordinary and laudable steps they take to protect consumers and carrier networks.[20] The Commission therefore should adopt a sufficiently broad call-blocking safe harbor to "encourage voice service providers to block one-ring scam calls," as well as other suspected illegal calls, as AT&T has long urged.[21]

Finally, AT&T continues to believe that greater enforcement activity is required to make a serious dent in the volume of illegal calls targeted to American consumers. Congress recognized as much in the TRACED Act. Section 5 of the TRACED Act directs the Commission and the U.S. Attorney General to establish an interagency working group for the general purpose of stepping up robocall enforcement efforts and for the express purpose, among others, of identifying ways to "encourage and improve coordination among Federal departments and agencies and States, and between States, in the prevention and prosecution of" TCPA

---

19 *NPRM* ¶ 2.
20 *See Call Blocking Declaratory Ruling* ¶ 35 n.79.
21 *NPRM* ¶ 17.

violations.[22] Likewise, Section 11 of the TRACED Act requires the Enforcement Bureau to share evidence of egregious illegal robocall activity with the Attorney General.[23]

AT&T appreciates the Commission's efforts to target illegal robocallers through enforcement, including by bringing attention to providers suspected of facilitating COVID-19 scams. Likewise, increased coordination is evident in the concurrent activity of the Enforcement Bureau and several state attorneys general against groups and individuals long suspected of facilitating a dangerous and longstanding healthcare fraud robocall scheme. There is more work to be done to bring law breakers to justice and, in so doing, deter mass calling schemes. AT&T stands ready, willing, and able to assist toward this worthy end.

CONCLUSION

Consistent with the foregoing discussion, AT&T urges the Commission to take appropriate action to enable enhanced protection of consumers and carrier networks from the harms caused by illegal one-ring calling schemes.

Respectfully submitted,

/s/ Amanda E. Potter
Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys

June 19, 2020

[22] TRACED Act § 5(b).
[23] *See id.* § 11(a).